Vergleich des Umgangs mit Privatheit bei Passport und Liberty Alliance

Wolfgang Wörndl, Johann Zehentner, Michael Koch

Technische Universität München
Fakultät für Informatik
Boltzmannstr. 3
D-85748 Garching b. München
{woerndl,zehentne,kochm}@in.tum.de

Abstract: Ein Identitätsmanagementsystem ermöglicht es dem Benutzer, verschiedene Identitäten zu definieren und zu wählen, in welcher Rolle er gegenüber dem Kommunikationspartner auftritt und welche Informationen er über sich offenbart. Das Ziel dieser Arbeit ist es, einen Überblick über existierende Anwendungen für Identitätsmanagement im Internet zu geben und diese hinsichtlich der Erfüllung von Privatheitsanforderungen zu untersuchen. Dazu geben wir zunächst einen Überblick über verschiedene Anwendungen für Identitätsmanagement im Internet. Dann definieren wir Privatheitsanforderungen für solche Anwendungen und evaluieren die beiden wichtigsten Systeme, Microsoft .NET Passport und das Liberty Alliance Projekt anhand dieser Anforderungen.

1 Einleitung

Die Entwicklung des Internet beruhte ursprünglich auf der Annahme, dass der Benutzer anonym bleibt bzw. es war nicht relevant, ob ein Benutzer anonym ist oder nicht. Durch die Verbreitung des Internets entwickelten sich aber immer mehr Dienste, die zur Erfüllung ihrer Aufgaben Informationen über ihre Anwender benötigen. Eine wichtige Funktionalität in diesem Zusammenhang ist die Personalisierung von Diensten und von Informationen. Um Personalisierung durchzuführen, muss eine Identifizierung der Benutzer und eine Beschaffung von Informationen zu diesen Benutzern über das Internet abgewickelt werden.

Im Zusammenhang mit der Identifikation von Benutzern und der Handhabung von Information zu den Benutzern wird häufig von Identität und Identitätsmanagement gesprochen. Das Webster English Dictionary erklärt das Wort „identity" als: „*1) the condition or fact of being the same or exactly alike (sameness, oneness); 2a) the condition or fact of being a specific person or thing (individuality); b) the condition of being the same as a person or thing described or claimed*" [We88]. Hinter Identität verbirgt sich also die Eigenschaft, eine bestimmte Person zu sein, und auch eine Menge von Informationen, die eine bestimmte Person näher beschreibt. Ersteres spielt eine Rolle bei der Authentifizierung von Benutzern im Internet, zweites definiert im Internet einige Anforderungen an die Autorisierung von Zugriffen, an das Identitätsmanagement.

Unter Identitätsmanagement versteht man dabei eine Festlegung und Durchsetzung, welche Informationen für welche Person oder Anwendung verfügbar sind. Identitätsmanagement betreiben wir tagtäglich wenn wir bei Gesprächen entscheiden, was wir unserem Gesprächspartner über uns selbst mitteilen. So können Personen in verschiedenen Kontexten unter verschiedenen Namen bekannt sein, z.B. durch die Nutzung spezieller Spitznamen oder von Pseudonymen [CK01, BK00]. Diese Flexibilität muss auch in Netzwerk-basierten Computersystemen zur Verfügung stehen. Anwendungen für Identitätsmanagement im Internet wie Microsoft .NET Passport sollen dies bereitstellen. Dazu realisieren diese Systeme eine Trennung der Benutzerprofilverwaltung von den nutzenden Diensten und eine dienstübergreifende Authentifizierung.

Das Ziel dieser Arbeit ist es, einen Überblick über existierende Anwendungen für Identitätsmanagement im Internet zu geben und diese hinsichtlich der Erfüllung von Privatheitsanforderungen zu untersuchen. Im ersten Teil des Beitrags listen wir dazu zuerst einige aktuell existierende Lösungen auf (Abschnitt 2). Der folgende Abschnitt 3 widmet sich dann dem Thema Privatheit und erarbeitet Anforderungen, die an Identitätsmanagementsysteme gestellt werden können. Anschließend erfolgt eine Evaluation der Anforderungen bei den beiden wichtigsten Vertretern der Anwendungsklasse, Microsoft .NET Passport und dem Liberty Alliance Projekt (Abschnitt 4). Der Artikel schließt mit einer kurzen Zusammenfassung und einem Ausblick. Dabei wird auch auf relevante und aktuelle Beiträge in der Wissenschaft hingewiesen.

2 Anwendungen für Identitätsmanagement im Internet

2.1 Funktionalitäten

Identitätsmanagementsysteme stellen in der Regel die folgenden Funktionalitäten zur Verfügung:

- Verwaltung verschiedener Identitäten und Ermöglichung anonymer und pseudonymer Kommunikation
- Verwaltung von Benutzerprofilattributen und Zugriffsrechten darauf (Autorisierung)
- Bereitstellung eines Single-Sign-On (SSO) Dienst (Authentifizierung)

Anwendungsgebiete von Identitätsmanagementsystemen sind z.B. das automatische Ausfüllen von Web-Formularen oder die Vereinfachung von Bestellung und Zahlungsabwickelung im Internet.

Kern vieler Identitätsmanagementsysteme ist der *Single-Sign-On (SSO)* Dienst (vgl. Abb. 1). Durch den *SSO* Dienst wird eine dienstübergreifende Authentifikation realisiert. Dies erfolg meist mit Hilfe von *http-Redirect* oder einem vergleichbaren Mechanismus.

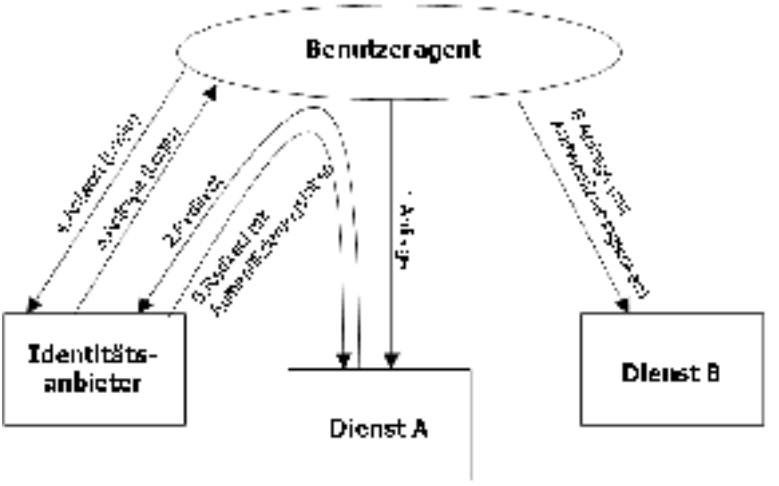

Abbildung 1: Single Sign On Protokoll

Dabei wird nach einer Anfrage eines Benutzeragenten (Web-Browser) ohne Authentifizierungsinformation ein „Redirect" zum Server des Identitätsanbieters veranlasst. Dieser authentifiziert den Benutzer, z.B. mit Hilfe einer Eingabe von Benutzernamen und Passwort, und führt einen weiteren Redirect zurück zum ursprünglichen Dienst durch (Schritt 5) mit einem Authentifizierungstoken, das i.d.R. als Cookie realisiert ist. Der Identitätsanbieter wird dabei nur eingeschaltet, wenn der Benutzeragent nicht in Besitz des Authentifizierungstokens ist. Nach einer erfolgten Authentifizierung kann das Token für eine automatische Anmeldung bei weiteren Diensten genutzt werden (vgl. Schritt 6).

2.2 Systeme und Einsatzgebiete

Dieser Abschnitt gibt einen Überblick über die derzeit wichtigsten Identitätsmanagementsysteme. Ein wichtiges Differenzierungsmerkmal der Anwendungen liegt im Grundkonzept. Man unterscheidet bei der Architektur zwischen server- und clientbasiert. Bei einem serverbasierten Ansatz werden persönliche Daten auf einem Server gespeichert, auf die der Benutzer z.B. über eine Web-Schnittstelle zugreifen kann, während bei einer clientbasierten Architektur zumindest Teile des Benutzerprofils oder Informationen über Kennungen auf dem Rechner des Benutzers abgelegt werden. Im Folgenden betrachteten wir Systeme, die jeweilige Architektur und die wichtigsten Dienste im Überblick.

Microsoft .NET Passport (www.passport.com) ist ein Teil der .NET („dot net") Infrastruktur. Es realisiert mit einem zentralen, serverbasierten Authentifizierungssystem einen SSO-Dienst basierend auf http-Redirect wie oben gezeigt. Passport verwaltet eine sehr große Menge an Kennungen, da z.B. jeder Benutzer des kostenlosen Email-Dienstes Hotmail von Microsoft automatisch eine Passport-Kennung hat.

Das *Liberty Alliance* Projekt (www.projectliberty.org) ist eine Vereinigung von ca. 120 Firmen wie AOL, Mastercard oder Sun Microsystems mit dem Ziel, einen offenen Standard als Grundlage zur Realisierung eines SSO-Dienstes und Möglichkeiten zum Austausch von Authentifizierungs-, Autorisierungs- und Benutzerprofilinformationen zu definieren. Der Ansatz sieht im Gegensatz zu .NET Passport eine verteilte, föderierte Benutzerprofilverwaltung (vgl. Abschnitt 4.2.) vor.

Extensible Name Service (XNS) (www.xns.org) stellt eine offene Plattform bereit, die eine Definition und Verwaltung von Identitäten und Beziehungen zwischen diesen erlaubt. Dies ist vergleichbar mit der Liberty Alliance Spezifikation. Darauf aufbauend wird ein SSO-Dienst und ein automatisches Ausfüllen von Web-Formularen realisiert.

Novell digitalme (www.digitalme.com) bietet einen Verzeichnisdienst, eine Verwaltung verschiedener Identitäten eines Benutzers mit zugehörigen Profilinformationen und Funktionalitäten wie einem clientseitigen, automatischem Ausfüllen von Web-Formularen. Neben einem SSO-Dienst stellt *Yodlee* (www.yodlee.com) eine Verwaltung von verschiedenen Online-Banking-Konten sowie kontenübergreifende zusammenfassende Informationen bereit. Yodlee hat den Schwerpunkt auf einer übersichtlichen Verwaltung von persönlichen Daten für den Benutzer, dazu kann die Menge der gespeicherten Attribute erweitert werden.

Eine clientbasierte Lösung zum SSO bietet *PingID* (www.pingid.com). Die Lösung stellt ferner ein Open Source Framework für Entwickler bereit, mit dem eigene Anwendungen um Identitätsmanagement-Funktionalität erweitert werden können (vgl. www.pingid.org bzw. www.sourceid.org). PingID hat im Gegensatz zu den meisten anderen Anwendungen den Fokus stärker auf einer Benutzer-zu-Benutzer Beziehung. Nur die Authentifikation wird über eine vertrauenswürdige dritte Partei abgewickelt. Dies ermöglicht eine Form von „persönlichem Identitätsmanagement“ [Dy02].

Infospace (www.infospace.com) bietet dem Benutzer neben der Verwaltung von Profildaten über eine clientseitige Anwenderkonsole (vgl. Abb. 3) auch eine Dokumenten- und Geräteverwaltung und ermöglicht eine Synchronisation der Daten mit anderen Anwendungen wie dem Email-Programm Microsoft Outlook.

Abbildung 2: Infospace Konsole

Es gibt darüber hinaus einige Unternehmen, wie z.B. *Persona* (www.persona.com), die Produkte zur Personalisierung von Web-Seiten, zum Email Marketing oder der Unterstützung von Customer Relationship Management (CRM), anbieten. Dabei werden auch SSO und andere Funktionalitäten eines Identitätsmanagements angeboten, z.T. auch Möglichkeiten für den Benutzer bzw. Kunden eine Verwendung von personenbezogenen Daten zu kontrollieren.

Open Privacy (www.openprivacy.org) realisiert schließlich in einem (Teil-)Projekt *User Content License* u.a. ein sog. „Reversing the Privacy Policy Circle“. Dabei wird der Benutzeranfrage ein http-Header angefügt, der Informationen über einen Copyright-Schutz von Benutzerdaten enthält. Damit sollen vor einer möglichen Datenübermittlung vom Client zum Server die Bedingungen eines Datenzugriffs festgelegt werden.

Aus Sicht der Privatheit ist dies allerdings eher bedenklich, da mit der Übertragung von Benutzerpräferenzen an einen Dienst bereits ein wesentlicher Verlust von Privatheit verbunden ist. In Kapitel 4 werden weitere Aspekte hinsichtlich Sicherheit und Privatheit bei den beiden wichtigsten Anwendungen dargestellt. Dazu werden zunächst einige Anforderungen definiert.

3 Anforderungen für Privatheit

Unter *Privatheit* (engl. privacy) versteht man nach Alan Westin: „*Privacy is the claim of individuals, groups or institutions to determine for themselves, when, how and to what extent information about them is communicated to others.*“ (aus: [We67]). Essentiell ist dabei der Aspekt der Kontrolle des Benutzers über die Sammlung und Verwendung seiner personenbezogenen Daten. Des Weiteren gibt es gesetzliche Regelungen und Richtlinien für Datenschutz auf nationaler und z.T. auch internationaler Ebene, auf die hier nicht weiter im Detail eingegangen werden kann, eine Sammlung einiger Verweise dazu findet sich z.B. unter www.datenschutzzentrum.de/ldsh/gesetze.htm.

3.1 Klassische Schutzziele

Zuerst sind hier die klassischen Schutzziele von elektronischer Kommunikation, Vertraulichkeit, Zurechenbarkeit und Integrität zu erwähnen. Bezüglich des Austausches personenbezogener Daten ist außerdem *Datensparsamkeit* zu fordern, d.h. die Erhebung einer minimalen zur Diensterfüllung nötigen Teilmenge der personenbezogenen Informationen, sowie ggf. die Möglichkeit der Verwendung eines Pseudonyms. Ein weiterer Aspekt ist die *Autorisation* einer Datenverwendung durch den Benutzer. Diese Möglichkeit für den Benutzer, selbst und feingranular zu beeinflussen, welche Dienste welche Daten erhalten können, zeichnet benutzerzentrierte Identitätsmanagementsysteme aus. *Verfügbarkeit* gehört auch zu den klassischen Schutzzielen, ist jedoch aus Sicht der Privatheit weniger relevant.

3.2 Technische Systemanforderungen

Die klassischen Schutzziele müssen technisch durchgesetzt werden. Ein Aspekt dabei ist der Zugriffschutz auf die persönlichen Profildaten. Dieser Schutz wird durch ein Authentifizierungssystem sichergestellt. Ein geeignetes System sieht dazu die Verwendung eines Authentifikators vor, der z.B. durch ein digitales Zertifikat realisiert werden kann.

Eine zeitliche Beschränkung von Authentifizierungsinformationen ist sinnvoll. Ein unerlaubter Zugriff muss die Offenlegung von Authentifizierungs- und Profildaten (im Rahmen der Diensterfüllung) minimieren, was durch eine gemeinsame, dienstübergreifende Profildatennutzung unterstützt werden kann. Für ein Identitätsmanagementsystem muss Erweiterbarkeit und Konfigurierbarkeit gefordert werden, um für den Einsatz neuer Protokolle vorbereitet zu sein und eine benutzerspezifische Auswahl von z.B. digitalen Signaturen oder Zertifikaten zu ermöglichen.

3.3 Datenschutzerklärung

Die Praktiken in Bezug auf Datenschutz und Privatheit werden üblicherweise in einer *Datenschutzerklärung* (engl. privacy policy) festgehalten. Die Verfügbarkeit einer Datenschutzerklärung, der Dienste, die persönliche Daten speichern und verarbeiten, ist deshalb eine wichtige Anforderung, damit der Benutzer eine informierte Entscheidung treffen kann, ob er persönliche Daten herausgeben will oder nicht. Eine Unterstützung des W3C Standards *Platform for Privacy Preferences Project (P3P)* zur Ermöglichung einer automatischen Auswertung der Erklärung ist wünschenswert.

Es ist es außerdem wichtig, dass die Einhaltung der Datenschutzerklärungen durch unabhängige, von der Industrie anerkannte Organisationen überprüft wird. Werden zwischen Dienstanbieter und -nutzer Verträge vereinbart, tritt der Aspekt der Sicherheitsgarantie in den Vordergrund. Um obiger Definition gerecht zu werden, müssen Benutzerkontrolle und „Opt-In“ Auswahl (d.h. der Benutzer muss einer Datenverwendung explizit zustimmen), sowie angemessene Präsentation sichergestellt sein.

3.4 Benutzerschnittstelle

Die Gestaltung der Benutzerschnittstelle stellt im Hinblick auf Selbstbeschreibungsfähigkeit, Individualisierbarkeit sowie Fehlervermeidung und -toleranz einen wichtigen Teil eines Identitätsmanagementsystems dar. Sichere Defaulteinstellungen sowie Korrektheit und Eindeutigkeit der Anzeige sind deshalb unabdingliche Privatheitsanforderungen. Die Benutzerschnittstelle muss dem Anwender die volle Kontrolle über seine Daten und deren Weitergabe an Dritte bzw. deren Weiterverwendung durch den Dienst gewährleisten. Die Benutzerschnittstelle muss den Anwender über die Datenverwendung informieren, d.h. Transparenz bieten und durch ein geeignetes Überwachungssystem aussagekräftige Sicherheitswarnungen generieren können.

4 Evaluierung ausgewählter Systeme

In diesem Abschnitt werden Microsoft .NET Passport und die Spezifikation des Liberty Alliance Projektes näher hinsichtlich Privatheit betrachtet.

.NET Passport hat die größte Verbreitung in der Praxis und war bereits einer Reihe von Angriffen ausgesetzt. Der offene, föderierte Ansatz der Liberty Alliance könnte in der Zukunft eine wichtige Rolle beim Identitätsmanagement im Internet spielen. Eine ausführlichere Darstellung der folgenden Evaluierung der beiden genannten und weiterer Systeme und der durchgeführten Tests ist in [Ze02] zu finden. In einem Arbeitspapier zu Online-Authentifizierungsdienste der „Artikel-29-Datenschutzgruppe“ [Eu02, Eu03] wird auch auf Datenschutz-Probleme von Microsoft .NET Passport und Liberty Alliance eingegangen und auf notwendige Verbesserungen hingewiesen.

4.1 Microsoft .NET Passport

4.1.1 Datenerhebung, Datenweitergabe und Benutzerkontrolle

Bei einer Neuanmeldung an einem .NET Passport Dienst kann der Benutzer angeben, ob die Email- Adresse und weitere Registrierungsdaten (z.B. Land oder Sprache) mit anderen Diensten geteilt werden sollen. Die Auswahl kann man später relativ leicht wieder rückgängig machen. Eine Weitergabe von Benutzerdaten erfolgt nur an Passport Partnersites. Eine genauere Unterteilung, an welche Dienste welche Informationen gegeben werden, ist aber nicht möglich. Auch wird der Benutzer nicht benachrichtigt oder in sonstiger Weise informiert, wenn neue Passport Partner hinzukommen und somit Zugriff auf die Daten haben.

Eine detaillierte Autorisierung durch eine Vergabe von Zugriffsrechten für einzelne Profilattribute ist nicht vorhanden. Für die Anforderung einer geeigneten Benutzerkontrolle ist das System damit zu wenig transparent, es fehlen Sicherheitswarnungen und genauere Angaben über die Profildatenverwendung.

Bezüglich der Datenschutzerklärung unterstützt Microsoft .NET Passport den P3P-Standard und unterwirft sich der Kontrolle der Datenschutzrichtlinien durch die Organisation TRUSTe. Policy-Änderungen werden auf der Homepage bekannt gegeben, eine explizite Benachrichtigung der Benutzer erfolgt jedoch nicht. Ein weiterer wichtiger Punkt hinsichtlich der Datenschutzerklärung sind Haftbarkeitsgarantien. Diese sind bei .NET Passport abhängig von den Beziehungen der implementierenden Organisationen zu Microsoft oder strategischen Partnern. Damit ein Anwender über die Menge der erhobenen Daten und deren Verwendung sicher sein kann, müssen neben der Datenschutzerklärung von .NET Passport also auch die Datenschutzerklärungen aller Partnersites geprüft werden.

4.1.2 Authentifizierung

Die Benutzeranmeldung bei einer Partnersite von .NET Passport basiert auf einem von .NET Passport an die Partnersite übermittelten verschlüsselten Identifikator. .NET Passport basiert bei der Authentifizierung auf proprietären Protokollen, wobei Cookies als Authentifizierungstokens benutzt werden. Der inhärente Schwachpunkt dieser Technik aus Sicht von Sicherheit und Privatheit liegt darin, dass alleine der Besitz des Authentifizierungstokens für eine Benutzeranmeldung ausreichend ist.

Die Authentifizierung mit http-Redirect und Cookies birgt insbesondere zwei Sicherheitsrisiken:

- Abhören der übertragenen Daten, wenn die Übertragung nicht mit SSL o.ä. gesichert wird
- Gefahr der Verwendung von gestohlenen Authentifizierungscookies

Eine bessere Lösung bietet z.B. ein Authentikator, wie er in Kerberos zum Einsatz kommt. Eine Integration von Kerberos in .NET Passport ist für 2003 angekündigt[1].

Bei der Registrierung eines Dienstes als Partnersite kann dieser zwischen drei Sicherheitsstufen wählen, wobei bei der niedrigsten Stufe keine Sicherheitsanforderungen verlangt werden. Die Sicherheitsstufe einer Passport Partnersite ist nicht ersichtlich für den Benutzer, was eine wichtige Information für den Benutzer wäre.

Während der Anwendung von .NET Passport treten sporadische Fehler auf (vgl. Abb. 3 aus [Ze02]). Ein Abmelden von einer Partnersite müsste die Abmeldung von allen Partnersites, bei denen der Benutzer angemeldet ist, mit sich ziehen. Dies ist durch den Dienst jedoch nicht garantiert und führt somit zu Einschränkungen der Benutzerkontrolle und der Vertraulichkeit sowie der Anforderungen der Korrektheit, der Eindeutigkeit und der geeigneten Sicherheitswarnungen. Eine detaillierte Durchführung und Bewertung systematischer Tests ist in [Ze02] zu finden.

Abbildung 3 Abmeldeproblem bei Passport

[1] Vgl. dazu z.B. www.computerworld.com/securitytopics/security/story/0,10801,75764,00.html

4.1.3 Angriffspunkte und Sicherheitsrisiken

Einige Sicherheitsprobleme von .NET Passport wurden von Kormann und Rubin in [KR00] aufgezeigt, auf die hier nicht im Detail eingegangen werden kann. Darunter fallen Probleme des Schlüssel-Managements, da zur Verschlüsselung aller Authentifizierungstokens nur ein Serverschlüssel verwendet wird.

Auch stellt der zentralisierte Ansatz von Passport ein potentielles Angriffsziel dar und ermöglicht Denial of Service Attacken. Des Weiteren könnten böswillige Sites eine Zugehörigkeit zu Passport (z.B. durch Wahl einer Domäne wie pasport.com) vortäuschen und dabei an Authentifizierungsdaten unaufmerksamer Benutzer herankommen.

Obgleich einige der Sicherheitslücken mittlerweile von Microsoft behoben oder gelindert wurden, zeigt sich zusammenfassend doch, dass das Konzept von Passport nur wenig auf Sicherheit und Privatheit ausgerichtet ist.

4.2 Liberty Alliance Projekt

Im Gegensatz zu Microsoft .NET Passport ist Liberty Alliance kein Dienst, sondern eine Spezifikation für Schnittstellen von Diensten, die gemeinsam einen föderierten Identitätsmanagementdienst anbieten. Direkt vergleichbar zu Passport wäre also eine konkrete Implementierung und Instantiierung der Liberty Alliance Spezifikation. Derzeit unterstützt der Sun Identity Server 6.0 als einziges kommerzielles Produkt die Liberty Alliance Spezifikation.

4.2.1 Datenerhebung, Datenweitergabe und Benutzerkontrolle

Liberty Alliance legt in der Spezifikation die Kommunikation zwischen den am Single Sign On Dienst beteiligten Akteuren – Benutzer, Identitätsanbieter und Dienstanbieter – fest. Ein Identitätsanbieter ist dabei ein Netzwerkzugangspunkt, der die Benutzerauthentifizierung für den Zugang zu einem Dienstanbieter übernimmt. Ein Identitätsanbieter kann zudem selbst auch als Dienstanbieter agieren. Die Benutzerauthentifizierungsdaten werden dabei dezentral bei den Identitätsanbietern gespeichert. In dem durch Liberty Alliance aufgespannten Netz verbundener Anbieter und Benutzer existiert im Gegensatz zu .NET Passport keine global eindeutige Benutzer-ID.

Liberty Alliance spezifiziert die Verbindung von Identitäten (sog. „identity federation“), also von Benutzerkonten. Ein Benutzer kann explizit auswählen, welche seiner Konten bei verschiedenen Dienstanbietern und Identitätsanbietern verbunden werden sollen. Die Spezifikation legt bei der Verbindung von Identitäten eine Restriktion fest, nach der nur direkte Verbindungen zum Austausch von Authentifizierungsdaten genutzt werden können. Der Privatheitsgewinn liegt darin, dass durch die Offenlegung einer Benutzeridentität keine weiteren verbundenen Identitäten enthüllt werden.

Durch den Einsatz von SAML (Security Assertion Markup Language) und einer Datenschutzerklärung basierend auf einer Opt-In-Auswahl ist die Benutzerkontrolle über die Authentifizierungsdaten gewährleistet [Ze02]. Im Gegensatz zu Microsoft .NET Passport liegt bei Liberty Alliance die Haftbarkeit bei den Organisationen, die die Beziehungen untereinander erzeugen. Identitätsanbieter und Dienstanbieter sind somit direkt an datenschutzrechtliche Verantwortung gebunden, wodurch die Privatheitsanforderung nach Sicherheitsgarantien erfüllt ist.

Derzeit sind keine Mechanismen für eine Autorisation von Benutzerprofilzugriffen in der Liberty Alliance Spezifikation enthalten, dies ist aber für zukünftige Versionen vorgesehen. Neben der auf Zugriffsrechten basierenden gemeinsamen Nutzung von Profilattributen ist für 2003 auch eine Leitfaden zur Site-to-Site-Authentifizierung für SAML-Assertions, Kerberos-Tickets und PKI-basierte Technologien geplant.

4.2.2 Authentifizierung

Eine Menge von Identitätsanbietern speichern verteilt die Benutzerauthentifizierungsinformationen in Form von Tokens und tauschen diese bei der Verbindung der Identitäten unter Verwendung von http-Redirect und SAML aus.

Liberty Alliance definiert hier zum einen eine Subklassenbildung von Informationen und Formaten, wie diese zwischen Dienstanbieter und Identitätsanbieter ausgetauscht werden. Subklassen sind die Identität, der Authentifizierungskontext sowie Informationen zu den Dienstanbietern. Auf diese Weise wird zum einen der Forderung nach Datensparsamkeit Rechnung getragen [Ze02]. Zum anderen ermöglicht der Authentifizierungskontext Identitäts- und Dienstanbietern eine Auswahl des zu verwendenden Authentifizierungsmechanismus, stellt also ein Mittel zur Erweiterbarkeit des Systems dar. Zur Benutzeranmeldung kann zudem ein X.509 Zertifikat herangezogen werden, d.h. Liberty Alliance unterstützt das Konzept eines Authentifikators zur Benutzerauthentifizierung. Die innerhalb einer Menge von vertrauenswürdigen Anbietern („circle of trust“) beteiligten Instanzen können somit eine Auswahl der zu verwendenden Mechanismen treffen, abhängig vom gewünschten Sicherheitsgrad und Authentifizierungstyp. Allerdings wird die Menge der einsetzbaren Mechanismen nicht auf eine konkrete Auswahl beschränkt, wodurch unsichere Authentifizierungssysteme zum Einsatz kommen können [Ze02].

4.2.3 Angriffspunkte und Sicherheitsrisiken

Die Verbindung vieler lokaler Identitäten mit vielen Dienst- bzw. Identitätsanbietern birgt (nach Liberty Alliance) ein Privatheitsrisiko, da dies zur Generierung einer großen Menge potentieller Authentifizierungsinformationen für einen Benutzer führt. Ein Identitätsanbieter, der in Besitz von diesen Informationen ist, kann damit bei jedem Dienstanbieter unter falscher Identität auftreten. Eine große Menge von lokalen Authentifizierungsinformationen eines Benutzers unterstützt diesen Effekt, da ein Missbrauch ungenutzt gespeicherter Authentifizierungsdaten nicht offensichtlich ist. Aus diesem Grund weist Liberty Alliance auf die Notwendigkeit eines Kontrollsystems zur Beschränkung dieser Authentifizierungsinformationen bzw. deren Gültigkeit hin. Mechanismen hierfür werden allerdings nicht spezifiziert.

Die Spezifikation von Liberty Alliance sieht die Verbindung verschiedener Authentifizierungssysteme unterschiedlicher Anbieter basierend auf einer dezentralen Authentifizierungsdatenhaltung vor. Deshalb ist eine Anwendung, die die Liberty Alliance Spezifikation implementiert, im Gegensatz zu Microsoft .NET Passport weniger durch Denial of Service Attacken gefährdet und die Verfügbarkeit ist kein zentrales Risiko [Ze02].

Liberty Alliance spezifiziert u.a. die Verwendung von http-Redirect und ermöglicht damit zwei potentielle Angriffspunkte. Das sind, wie bei .NET Passport, das Abhören der Daten auf der Übertragungsstrecke und die unerlaubte Verwendung von gestohlenen Authentifizierungstokens.

Um den Anforderungen der Vertraulichkeit und der Verdecktheit gerecht zu werden, stellt Liberty Alliance mit der Spezifikation die nötige Infrastruktur bereit. Allerdings werden keine Sicherheitsmechanismen spezifiziert, die zur Erfüllung dieser Schutzziele zum Einsatz kommen müssen, was Sicherheitslücken in den Implementierungen zulässt [Ze02].

5 Zusammenfassung und Ausblick

Die Systeme zum Identitätsmanagement fokussieren auf einer dienstübergreifenden Authentifikation, oftmals basierend auf Single Sign On mit HTTP-Redirect und bieten zusätzliche Funktionalitäten für den Benutzer. SSO ist eine Erleichterung für den Benutzer, aber bietet wenig Vorteile hinsichtlich Sicherheit oder Privatheit, eher im Gegenteil, da Sicherheitsprobleme vorhanden sind und die Übersicht und Transparenz für den Benutzer leiden kann. Microsoft hat sich nach Gesprächen mit der „Artikel-29-Datenschutzgruppe“ verpflichtet, innerhalb eines vereinbarten Zeitplans wesentliche Änderungen an Passport vorzunehmen, auf die im Arbeitspapier der Gruppe [Eu03] hingewiesen wurde.

In dieser Arbeit wurde zunächst ein Überblick über Anwendungen für Identitätsmanagement im Internet gegeben. Danach wurden die zwei wichtigsten Ansätze zum Identitätsmanagement, Microsoft .NET Passport und das Liberty Alliance Projekt, näher hinsichtlich definierter Privatheitsanforderungen untersucht. Die Verwendung personenbezogener Daten durch Identitätsmanagementanwendungen macht den Einsatz von Mechanismen zur Benutzerkontrolle sowie zum Schutz dieser Daten und zur Visualisierung und Warnung des Benutzers erforderlich.

Zusammenfassend lässt sich festhalten, dass ein stärkerer Fokus hinsichtlich Privatheit notwendig ist. Eine detaillierte Autorisation von Diensten zum Zugriff auf personenbezogene Daten fehlt bei den Anwendungen für Identitätsmanagement noch weitgehend. Die Liberty Alliance Spezifikation ist als gute Ausgangsbasis für eine sichere und benutzerzentriertes Authentifikation zu sehen. Es bleibt abzuwarten, inwieweit sich die Liberty Alliance Spezifikation gegen Microsoft .NET Passport behaupten kann. Derzeit ist eine Interoperabilität technisch wegen unterschiedlicher Details bei der Authentifikation nicht möglich.

Aktuelle Arbeiten der Wissenschaft behandeln solche Aspekte. So wird zum Besipiel in [Wö03, KW01] ein Ansatz zu einem benutzerzentrierten Identitätsmanagement und zur Autorisation von Benutzerprofilzugriffen mit Zugriffstokens vorgestellt. Im Projekt ATUS [JM00] wird ein Modul zur Unterstützung des Benutzers bei der Wahrnehmung von Identitätsmanagementfunktion entwickelt. Des Weiteren wird in [CPH02] auf eine Architektur für ein datenschutzkonformes Identitätsmanagement und einige dabei wichtige Aspekte eingegangen.

Literaturverzeichnis

[BK00] Berthold, O.; Köhntopp, M.: Identity Management Based On P3P. In: Workshop on Design Issues in Anonymity and Unobservability; Berkeley CA; Jul. 2000

[CK01] Clauß, S.; Köhntopp, M.: Identity Managements and Its Support of Multilateral Security. In: Computer Networks 37 (2001), Special Issue on Electronic Business Systems; Elsevier, North-Holland; S. 205-219

[CPH02] Clauß, S; Pfitzmann, A.; Hansen, M: Privacy-Enhancing Identity Management. IPTS Report; Vol. 67; 2002

[Dy02] Dyson, E.: Personal Identity Management: The Applications; Release 1.0; Vol. 20 No. 7; Jul. 2002

[Eu02] Erste Orientierungen der Artikel 29 Datenschutzgruppe zu on-line Authentifizierungsdiensten – Arbeitsdokument; Verfügbar unter: http://europa.eu.int/comm/internal_market/privacy/workingroup/wp2002/wpdocs02_de.htm

[Eu03] Arbeitspaper zu Online-Authentifizierungsdiensten der Artikel 29 Datenschutzgruppe; Verfügbar unter: http://europa.eu.int/comm/internal_market/privacy/workingroup/wp2003/wpdocs03_de.htm

[KW01] Koch, M.; Wörndl, W.: Community Support and Identity Management, Proc. European Conf. on Computer-Supported Cooperative Work (ECSCW2001), Bonn, Sep. 2001, S. 319 – 338.

[KR00] Kormann, D. P.; Rubin, A. D.: Risks of the Passport Single Signon Protocol. In: IEEE Computer Networks; Vol. 33; 2000

[JM00] Jendricke, U.; Markotten, G. tom: Usability meets Security – The Identity-Manager as your Personal Security Assistant for the Internet. In: Proc. 16th Annual Computer Security Applications Conference; New Orleans, USA; 2000.

[We88] Webster's New World Dictionary of American English; Third College Edition; Cleveland; 1988

[We67] Westin, A.: Privacy and Freedom; New York; 1967

[Wö03] Wörndl, W.: Privatheit bei dezentraler Verwaltung von Benutzerprofilen; Dissertation; Fakultät für Informatik, Technische Universität München, 2003

[Ze02] Zehentner, J.: Privatheit bei Anwendungen für Identitätsmanagement im Internet; Diplomarbeit; Fakultät für Informatik, Technische Universität München; Dez. 2002